UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/776,406	02/10/2004	Steven A. Crosson Smith	BT-027	2425

29956 7590 07/24/2007

TIMOTHY P. O'HAGAN
8710 KILKENNY CT
FORT MYERS, FL 33912

EXAMINER	
KAMAL, SHAHID	
ART UNIT	PAPER NUMBER
3609	

MAIL DATE	DELIVERY MODE
07/24/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/776,406	CROSSON SMITH, STEVEN A.	
	Examiner	Art Unit	
	Shahid Kamal	3609	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-17 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-17 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 02/10/2004 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cook et al. (US Patent No. 6,675,153 B1) in view of Yacobi et al. (US Patent No. 7,020,638 B1).

3. Referring to claim 1. Cook et al. disclose a digest by performing a hash on the electronic fund transfer disbursement file (col. 1, lines 24-41);

- Receiving an authorization response from the remote system (col. 2, lines 39-55);
- A web server system for transferring authorization control code to the remote system, the authorization control code driving the remote system to perform the following steps (Fig. 4). In the fig. 4 shows the web server, which is well known to do this kind of operations.
- Obtaining the digital signature of authenticated attributes, the authenticated attributes including the digest (col. 2, lines 38-52);
- And generating the authorization response, the authorization response including the digital signature (col. 2, lines 38-52).

Cook et al. does not expressly disclose a payment management system for obtaining approval of an electronic fund transfer disbursement file from a user of a remote system and transferring

the electronic fund transfer disbursement file to a payments processor, the payment management system comprising: an electronic transfer submission module for; transferring an electronic funds submission to the payments processor, the electronic funds submission comprising the payment transaction file and at least a portion of the authorization response comprising a digital signature;

Yacobi et al. discloses a payment management system for obtaining approval of an electronic fund transfer disbursement file from a user of a remote system and transferring the electronic fund transfer disbursement file to a payments processor, the payment management system comprising (col. 1, 5, lines 24-44, 50-57):

- An electronic transfer submission module for (col. 5, line 50-57):
- Transferring an electronic funds submission to the payments processor, the electronic funds submission comprising the payment transaction file and at least a portion of the authorization response comprising a digital signature (col. 16, 18, lines 8—14, 54-67);

Therefore, at the time the invention was made, it would have been obvious to a person of ordinary skill in the art to have modified of Cook et al. to include the step(s) taught by Yacobi et al. as discussed above in order to provide a real-time software application is provided that allows consumers to authorize transaction in a secure, private, and convenient manner for the purchase of goods and services over the internet (col. 1, lines 52-56).

4. Referring to claim 2. Cook et al. discloses the digital signature comprises a digital signature of a hash of the authenticated attributes (col. 1, lines 24-41).

- The authorization control code further provides for the remote system to, generate additional message attributes (col. 1, lines 24-41).

- Combine the additional message attributes with the digest to generate the authenticated attributes (col. 1, lines 24-41);

5. Referring to claim 3. Cook et al. discloses the authorization control code further drives the remote system to (col. 1, lines 14-49):

- Generate and pass a dummy data string to a signing component to obtain a dummy authentication data structure, the dummy authentication data structure comprising a dummy digital signature (col. 1, lines 14-49);
- Pass the authenticated attributes to the signing component to obtain the digital signature (col. 1, lines 14-49);
- Combine the digital signature with at least a portion of the dummy authentication data structure by replacing the dummy digital signature with the digital signature to generate an authentication data structure (col. 1, lines 14-49);
- And include the authentication data structure in the authorization response (col. 1, lines 14-49).

6. Referring to claim 4. Cook et al. discloses the dummy data structure further comprises a dummy digest (col. 1, lines 14-49);

- The authorization control code further drives the remote system to combine the digest with the dummy authentication data structure to generate the authentication data structure by replacing the dummy digest with the digest (col. 1, lines 14-49).

7. Referring to claim 5. Cook et al. discloses a log on module for authenticating the user of the remote system by (col. 1, lines 14-49):

- Obtaining log on credentials identifying the user of the remote system; determining whether the log on credentials match those of an authorized user (col. 1, lines 14-49);
- The electronic fund transfer submission module transfers the authorization request to the remote system only if the log on credentials match those of an authorized user (col. 1, lines 14-49).

8. Referring to claim 6. Cook et al. discloses the electronic fund transfer submission module further authenticates the user of the remote system to the payments processor by (col. 1, lines 14-49):

- Receiving an authentication challenge from the payments processor (col. 1, lines 14-49);
- Transferring the authentication challenge to the remote system (col. 1, lines 14-49);
- Receiving an authentication response from the remote system; and transferring the authentication response to the payments processor (col. 1, lines 14-49).

9. Referring to claim 7. Cook et al. discloses an payment management system for obtaining an approval of an electronic fund transfer disbursement file from a user of a remote system and transferring the electronic fund transfer disbursement file to a payments processor, the payment management system comprising (col. 1, 2, lines 14-49, 39-55):

- Means for generating a digest by performing a hash on the electronic fund transfer disbursement file (col. 1, 2, lines 14-49, 39-55);
- Means for transferring the digest to the remote system (col. 1, 2, lines 14-49, 39-55);
- Means for receiving an authorization response from the remote system, the authorization response comprising a digital signature of authenticated attributes, the authenticated attributes comprising the digest (col. 1, 2, lines 14-49, 39-55);

Cook et al. does not expressly disclose means for transferring an electronic funds submission to the payments processor over a secure connection, the electronic funds submission comprising the payment transaction file and at least a portion of the authorization response comprising the digital signature.

Yacobi et al. discloses means for transferring an electronic funds submission to the payments processor over a secure connection, the electronic funds submission comprising the payment transaction file and at least a portion of the authorization response comprising the digital signature (col. 3, lines 57-64).

Therefore, at the time the invention was made, it would have been obvious to a person of ordinary skill in the art to have modified of Cook et al. to include the step(s) taught by Yacobi et al. as discussed above in order to provide a real-time software application is provided that allows consumers to authorize transaction in a secure, private, and convenient manner for the purchase of goods and services over the internet (col. 1, lines 52-56).

10. Referring to claim 8. Cook et al. disclose the remote system comprises means for: generating additional message attributes (col. 2, lines 38-65);

- Combining the additional message attributes with the digest to generate the authenticated attributes (col. 2, lines 38-65);
- The digital signature comprises a digital signature of a hash of the authenticated attributes (col. 2, lines 38-65).

11. Referring to claim 9. Cook et al. discloses the remote system further comprises means for (col. 1, lines 14-49):

- Generating and passing a dummy data file to a signing component to obtain a dummy authentication data structure, the dummy authentication data structure comprising a dummy digital signature (col. 1, lines 14-49);
- Passing the authenticated attributes to the signing component to obtain the digital signature (col. 1, lines 14-49);
- Combining the digital signature with at least a portion of the dummy authentication data structure by replacing the dummy digital signature with the digital signature to generate an authentication data structure (col. 1, lines 14-49);
- Including the authentication data structure in the authorization response (col. 1, lines 14-49).

12. Referring to claim 10. Cook et al. discloses the dummy data structure further comprises a dummy digest (col. 1, lines 14-49);

- The remote system further combines the digest with the dummy authentication data structure to generate the authentication data structure by replacing the dummy digest with the digest (col. 1, lines 14-49).

13. Referring to claim 11. Cook et al. discloses the payment management system of claim 10, further comprising means for authenticating the user of the remote system by (col. 1, lines 14-49):

- Obtaining Iog on credentials identifying the user of the remote system; determining whether the Iog on credentials match those of an authorized user (col. 1, lines 14-49);
- Transferring the authorization request to the remote system occurs only if the Iog on credentials match those of an authorized user (col. 1, lines 14-49).

14. Referring to claim 12. Cook et al. discloses means for authenticating the user of the remote system to the payments processor by (col. 1, lines 14-49):

- Receiving an authentication challenge from the payments processor; transferring the authentication challenge to the remote system (col. 1, lines 14-49);
- Receiving an authentication response from the remote system; and transferring the authentication response to the payments processor (col. 1, lines 14-49).

15. Referring to claim 13. Cook et al. discloses a web server for passing authorization control code to the remote system, the authorization control code being at least one of executable by the remote system and interpretable by the remote system for driving the remote system to (col. 1, lines 24-41):

- Generate additional message attributes (col. 1, lines 24-41);
- Combine the additional message attributes with the digest to generate the authenticated attributes (col. 1, lines 24-41);
- The digital signature comprises a digital signature of a hash of the authenticated attributes (col. 1, lines 24-41).

16. Referring to claim 14. Cook et al. discloses the authorization control code further drives the remote system to (col. 1, lines 14-49):

- Generate and pass a dummy data file to a signing component to obtain a dummy authentication data structure, the dummy authentication data structure comprising a dummy digital signature (col. 1, lines 14-49);
- Pass the authenticated attributes to the signing component to obtain the digital signature (col. 1, lines 14-49);

- Combine the digital signature with at least a portion of the dummy authentication data structure by replacing the dummy digital signature with the digital signature to generate an authentication data structure (col. 1, lines 14-49);
- Include the authentication data structure in the authorization response (col. 1, lines 14-49).

17. Referring to claim 15. Cook et al. discloses the dummy data structure further comprises a dummy digest (col. 1, lines 14-49);

- The authorization control code further drives the remote system to combine the digest with the dummy authentication data structure to generate the authentication data structure by replacing the dummy digest with the digest (col. 1, lines 14-49).

18. Referring to claim 16. Cook et al. discloses means for authenticating the user of the remote system by (col. 1, lines 14-49):

- Obtaining Iog on credentials identifying the user of the remote system (col. 1, lines 14-49);
- Determining whether the Iog on credentials match those of an authorized user (col. 1, lines 14-49);
- Transferring the authorization request to the remote system occurs only if the Iog on credentials match those of an authorized user (col. 1, lines 14-49).

19. Referring to claim 17. Cook et al. discloses for authenticating the user of the remote system to the payments processor by (col. 1, lines 14-49):

- Transferring the authentication response to the payments processor (col. 1, lines 14-49).

Cook et al. does not expressly disclose receiving an authentication challenge from the payments processor; transferring the authentication challenge to the remote system; receiving an authentication response from the remote system.

Yacobi et al. discloses receiving an authentication challenge from the payments processor (col. 1, 5, lines 24-44, 50-57);

- Transferring the authentication challenge to the remote system; receiving an authentication response from the remote system (col. 1, 5, lines 24-44, 50-57).

Therefore, at the time the invention was made, it would have been obvious to a person of ordinary skill in the art to have modified of Cook et al. to include the step(s) taught by Yacobi et al. as discussed above in order to provide a real-time software application is provided that allows consumers to authorize transaction in a secure, private, and convenient manner for the purchase of goods and services over the internet (col. 1, lines 52-56).

Conclusion

20. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the patent examiner should be directed to Shahid Kamal whose telephone number is (571) 270-3272. The Patent examiner can normally be reached on Monday-Thursday (9:00am -7:00pm), Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Khoi Tran can be reached on (571) 272-6919. The fax phone number for this origination where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published application may be obtained from either Private PAIR or Public PAIR.

Statues information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-directed.uspto.gov.

Should you have any questions on accessing to the Private PAIR system, contact the Electronic Business Center (EBC) at 1(866) 217-9197 (toll free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 1(800) 786-9199 (IN USA OR CANADA) or 1(571) 272-1000.

Shahid Kamal
July 10, 2007

MATTHEW S. GART
PRIMARY EXAMINER
TECHNOLOGY CENTER 3600